

CLAIMS

What is claimed is:

*Suit
A1*

1 1. A hardware verification method comprising:
2 obtaining a set of packets to be driven by a device under test;
3 obtaining a set of timing and relation criteria which determines a sequence in
4 which the packets should be driven by the device under test;
5 starting multiple drive loops, each drive loop picking up a packet and forcing
6 the device under test to drive the packet;
7 starting multiple expect loops, each expect loop determining when to expect a
8 packet driven by the device under test and picking up the expected packet when it
9 arrives;
10 for each drive loop, confirming that the timing and relation criteria are satisfied
11 prior to allowing the drive loop to force the device under test; and
12 for each expect loop, checking if the expected packet arrives within a specified
13 time period and raising an error flag if the expected packet does not arrive within the
14 specified time period.

1 2. The method of claim 1 wherein allowing the drive loop to force the device
2 under test further includes obtaining permission to drive the device under test.

1 3. The method of claim 1 wherein determining when to expect a packet driven by
2 the device under test further includes determining if there is permission to drive the
3 device under test.

1 4. The method of claim 1 wherein the device under test is a bus bridge.

1 5. The method of claim 1 wherein the device under test is a data switch.

Sub
as

1 6. The method of claim 1 further including monitoring an output of the device
2 under test to determine whether a packet driven by the device under test is picked up
3 by one of the expect loops and raising an error flag if the packet is not picked up by
4 one of the expect loops.

1 7. The method of claim 1 wherein the expect and drive loops communicate over a
2 bus, the method further comprising monitoring activity on the bus and raising an error
3 flag if the bus is idle for more than a specified time period.

1 8. A hardware verification method comprising:
2 obtaining a set of packets to be driven by a device under test;
3 obtaining a set of timing and relation criteria which determines a sequence in
4 which the packets should be driven by the device under test;
5 starting multiple drive loops, each drive loop picking up a packet and forcing
6 the device under test to drive the packet;
7 starting multiple expect loops, each expect loop determining when to expect a
8 packet driven by the device under test and picking up the expected packet when it
9 arrives;
10 for each drive loop, confirming that the timing and relation criteria are satisfied
11 prior to allowing the drive loop to force the device under test;
12 for each expect loop, checking if the expected packet arrives within a specified
13 time period and raising an error flag if the expected packet does not arrive within the
14 specified time period; and
15 monitoring an output of the device under test to see if a packet driven by the
16 device under test is picked up by one of the expect loops and raising a flag if the
17 packet is not picked up by an expect loop.

*Sub
as*

1 9. The method of claim 8 wherein allowing the drive loop to force the device
2 under test further includes obtaining permission to drive the device under test.

1 10. The method of claim 8 wherein determining when to expect a packet driven by
2 the device under test further includes determining if there is permission to drive the
3 device under test.

1 11. The method of claim 8 wherein the device under test is a bus bridge.

1 12. The method of claim 8 wherein the device under test is a data switch.

1 13. The method of claim 8 wherein the expect and drive loops communicate over a
2 bus, the method further comprising monitoring activity on the bus and raising an error
3 flag if the bus is idle for more than a specified time period.

1 14. A hardware verification system, comprising:
2 at least one drive buffer for holding packets to be driven by a device under test;
3 at least one expect buffer for holding a set of timing and relation criteria which
4 determines a sequence in which the packets should be driven by the device under test;
5 a drive module which starts multiple drive loops that pick up packets from the
6 drive buffer and force the device under test to drive the packets, the drive module
7 ensuring that each drive loop satisfies specified timing and relation criteria prior to
8 allowing the drive loop to force the device under test; and
9 an expect module which starts multiple expect loops that pick up packets
10 driven by the device under test, the expect module ensuring that each expect loop
11 satisfies specified timing and relation criteria prior to allowing the expect loop to
12 expect and pick up a packet driven by the device under test, the expect module raising
13 an error flag if the expected packet does not arrive within a specified time period.

TOP SECRET//COMINT

Suff. cl.

1 15. The hardware verification system of claim 14 further including a spurious
2 packet checker module which starts a process that checks and raises an error flag if a
3 packet at an output of the device under test is not picked up by an expect loop.

1 16. The hardware verification system of claim 14 further including a controller
2 which controls communication between the drive loops, expect loops, and the device
3 under test.

1 17. The hardware verification system of claim 14 wherein the device under test is a
2 bus bridge.

1 18. The hardware verification system of claim 14 wherein the device under test is a
2 data switch.

1 19. The hardware verification system of claim 16 wherein the communication
2 occurs over a bus.

1 20. The hardware verification system of claim 19 further comprising a bus idle
2 monitor which monitors activity on the bus and sends an error notification to the
3 controller if the bus is idle for more than a specified time period.